

Re: Trojan/virus effects

Source: <http://www.derkeiler.com/Newsgroups/microsoft.public.security.virus/2004-06/1852.html>

From: Sandi – Microsoft MVP (sandi_hardmeier_at_mvps.org)

Date: 06/26/04

Date: Sat, 26 Jun 2004 18:26:51 +0800

There are many people who have helped this FAQ improve over time – MVPs and newsgroup users. I thank all of you who have made the newsgroups, anti-malware websites and dedicated mailing lists into such a wonderful resource.

Read the advice at my prevention link (<http://inetexplorer.mvps.org/data/prevention.htm>) to reduce the chances of your computer being infected.

IMPORTANT: Before trying to remove spyware, download a copy of LSPFIX from the URL below – some malware can kill your internet connection when it is removed, and this software should get things going for you again:
<http://www.cexx.org/lspfix.htm>

Also get a copy of WINSOCKFIX available at:
<http://www.spychecker.com/program/winsockxpfix.html>

The software you should download and have ready to use is:

AdAware – www.lavasoft.de [..Warning: AdAware is now version 6.181. All previous versions are NO LONGER SUPPORTED and will not be updated..]

Spybot Search and Destroy – <http://spybot.eon.net.au>

HijackThis – <http://209.133.47.12/~merijn/files/HijackThis.exe>

CWShredder – <http://www.merijn.org/files/CWShredder.exe>

IMPORTANT: After obtaining the required software above, make sure you check for updates and run the programmes in safe mode.

Malware removal (beginner's guide):

First, go to Control Panel, add/remove programs. Check for malware entries and use the uninstall programs, then reboot.

Go to start/run and type MSCONFIG. Go to the startup tab. Disable everything that you do not recognise as legitimate (do not disable any power

profile options).

Now go to the Services tab. Turn on the option to 'hide all Microsoft Services'. Disable everything that remains. If you don't have this option, don't worry about it.

Reboot your computer and hold down the F8 key until the boot menu options appear. Choose Safe Mode as your startup choice. You will find information about what safe mode is, and what it does, at this link [http://inetexplorer.mvps.org/data/safe_mode.htm]

Start CWSHREDDER. Update it, and fix anything it finds. Reboot back into safe mode.

Start AdAware. Use the 'check for updates now' op